1.0 PURPOSE:

To establish guidelines for the use of electronic message sending devices.

2.0 POLICY:

WHITCOM is equipped with systems that allow for the transmission of electronic mail, instant messages and terminal to terminal or multi-terminal message sending such as fax machines and the ACCESS or ILETS system. The system is intended for the enhancement of public safety, not for personal gain. Access to these systems is limited to WHITCOM Employees and members of the WHITCOM User Agencies. All other access except by expressed, written consent of the WHITCOM Executive Board is prohibited.

The Washington State Access System and Idaho State ILETS System are in place at WHITCOM, and applicable state rules and guidelines apply. Refer to ACCESS and ILETS Manual and SOP 550.

3.0 PROCEDURE:

3.1 Employees and user agencies may use all electronic message sending systems only for business related purposes only. All messages transmitted will include the name or personnel number of the sender and the name or number of the authorizing or requesting person if different. (Example: a teletype sent requesting information on a suspect might be signed “WHITCOM Miller for WSUPD Garrison”)

The message sending capabilities shall not be used for transmission of information that promotes:

3.1.1 Discrimination on the basis of age, gender, martial status, race, creed, color, national origin, sensory, mental or physical disability or sexual preference.

3.1.2 Sexual Harassment

3.1.3 Personal Political Views

3.1.4 Any unlawful activity

3.2 No one but trained, authorized employees of WHITCOM and members of the User Agencies shall access or otherwise make use of the systems.

3.3 No employee shall attempt, in any manner, to circumvent the security system of any WHITCOM system.

3.4 No employee shall tamper with, or attempt to repair, any hardware component for which he/she has not been specifically trained and assigned to maintain and/or repair.

3.5 No employee shall modify, reconfigure, add to, or delete from any software application, operating system or peripheral device unless specifically trained and assigned to do so.

3.6 No employee shall knowingly make a fictitious, unauthorized, unnecessary, anonymous, or inaccurate entry into the CAD system, data base, and/or mail/message handling system.

3.7 No employee shall knowingly make use of any computer terminal to which he/she is not logged on. [User Agencies refer to Section 5.0, User Agency Policy].

3.8 No employee shall make use of any other individual's security password for security access to any computer system.

3.9 Any employee who has cause to believe that the computer system security and/or integrity has been violated, compromised, or jeopardized, shall report same without delay to their Supervisor who will notify the Whitcom Director.

4.0 **RESPONSIBILITY**

4.1 Users have no expectation of privacy when utilizing any of the WHITCOM systems. Electronic messages cannot be protected against unauthorized access caused by:

4.1.1 User's failure to maintain password security
4.1.2 Devices logged onto the system but left unattended by Users
4.1.3 Messages forwarded to others by a recipient
4.1.4 Messages printed at locations where individuals other than the intended recipient may view.
4.1.5 Messages directed to the wrong recipient

4.2 Appropriate disciplinary action may be initiated against any employee who violates this policy.

4.2.1 It shall be the responsibility of the Supervisors to enforce, within reason, this policy and to monitor messages being sent by employees when necessary.

4.2.2 As part of an investigation, the WHITCOM Director shall take action to gather facts and may review and/or monitor messages being sent.

5.0 USER AGENCY POLICY

5.1 While WHITCOM does not have the authority or the desire to dictate User Agency policies or suggest disciplinary action, WHITCOM does reserve the right to restrict or deny system access should professional standards not be met by the Users.

5.1.1 Should the individual actions of a User necessitate potential limitations or denial of usage of the system, the severity of the violation[s] will determine whether a warning is issued to the User Agency or whether it is brought before the Executive Board for a decision to deny access.

5.1.2 An Agency may petition the Executive Board for a User's reinstatement to the system whenever they determine no further violations will occur.

5.2 No employee shall knowingly make use of any computer terminal to which he/she is not logged on.

6.0 MESSAGE TYPES

6.1 Terminal Messages: Electronic messages sent between specific ORI's using the ACCESS/ILETS/NCIC network. Terminal messages may only be transmitted or received on devices and over networks that meet the requirements of ACCESS/ILETS/NCIC and the current CJIS security requirements.

6.2 Spillman Messages / Mobile Messages: Electronic messages sent between Users of a single server, using the Spillman 'Message Center' or Spillman Email

6.3 Spillman Instant Messaging: A component of Spillman Mobile, similar in function to 'AOL Instant Messenger', 'Microsoft Messenger' and others but conducted on a private network, for real-time messages between users of a single Spillman server, using the Spillman Mobile or Spillman Message Center.

6.4 Spillman Message Center includes State Returns. All ACCESS/ILETS/NCIC messages will be located in the Message Center State Returns Folder.

6.5 Spillman Message Center includes a work flow folder. All work flow related messages will be located in the Message Center work flow folder.

7.0 INSTANT MESSAGING

7.1 Instant messages differ from regular e-mail messages in that they provide an opportunity for back-and-forth, instantaneous typed dialogue between two or more users.

7.1.1 Because of the conversational tone of instant messages, extra care must be taken by users to ensure that instant messages remain professional and contain appropriate content.

7.1.2 No communication through instant messenger should contain harassing, derogatory, sexually explicit or foul language.

7.1.3 Instant messenger communication is stored on the Spillman server and can be reviewed at any time.

7.1.4 Instant messages are subject to Public Disclosure and are discoverable; therefore, THERE IS NO EXPECTATION OF PRIVACY for any Instant Message communication.

7.2 Spillman Message Center users should not use instant messages to communicate with other users, especially dispatchers for anything that requires immediate attention.

7.2.1 Instant messages are the absolute lowest priority traffic transmitted over the Spillman system and should not be used to request items needing immediate action.